BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

18
18
36

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

3GPP TR 23.871 V2.10.0 (2002-

Technical Report

XP-002272724

3rd Generation Partnership Project; Technical Specification Group Services and System Aspects System Aspects;

Technical Report Enhanced support for User Privacy in location services (Release 5)

Keywords

UMTS, service, multicast

3GPP

Postal address

3GPP support office address

650 Route des Lucioles - Sophia Antipolis

Valbonne - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet

http://www.3gpp.org

Contents

Foreword 5

Introduction 5

1. Scope 6

2. References 6

3. Definitions, symbols and abbreviations 6

3.1 Definitions 6

3.2 Abbreviations 7

4. General description 7

5. Functional Description and Functional Requirements 7

5.1 Service Type Privacy 7

5.2 Support for enhanced privacy checking 8

5.3 Requestor 8

5.4 User Control 9

5.5 Codeword 9

5.7 Anonymity 10

5.8 Related privacy issues in Presence and Location services 10

5.9 Summary of enhanced user privacy in location services in Rel-5 and Rel-6 10

6. Network support for user privacy in Rel-5 11

6.1. Network support for Service Type and Codeword in Rel-5 11

6.2 Network support for Requestors in Rel-5 11

7. Network support for enhanced privacy checking in Release 6 11

7.1 Architecture alternative with privacy profile register (PPR) 13
7.1.1 Architecture 13
7.1.2 Information Flow 15

7.2. Architecture alternative with privacy profile register (PPR) attached to MSC/SGSN 15
7.2.1 Architecture 15
7.2.2 Information Flow 17
7.2.3 Exceptional handling 17

7.3. Architecture alternative with Home GMLC 17
7.3.1 Architecture 17
7.3.2 Information Flow 19

7.4 Architecture alternative with PPR associated with the HSS only 19

7.5 Comparison between each architectural alternatives 19

7.6 Conclusion on architecture for the enhanced privacy checking 23

8. Possible requestor enhancements in Rel-6 23

8.1 Architecture alternative with requestor authentication in GMLC 24

8.2 Backward compatibility 25

9. Stage 2 description of the anonymity concept 25

10. Charging Aspects 25

11. Security aspects 25

12. Roaming, Service Availability and Continuity 26

13. Conclusion 26

Annex A (informative): Change history 27

Foreword

This Technical Report has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

- x the first digit:
  - 1 presented to TSG for information;
  - 2 presented to TSG for approval;
  - 3 or greater indicates TSG approved document under change control.
- y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.
- z the third digit is incremented when editorial only changes have been incorporated in the document.

Introduction

There is a need to enhance the privacy mechanisms provided for Location Services to support the increasing number of LCS clients and the varying privacy requirements for location services. It should also be possible for the subscriber to set or change the location related privacy parameters in the home network. There are some limitations in support for user privacy in the current LCS specifications in 3GPP and there is a need to enhance the privacy mechanisms e.g. for roaming subscribers.

1. Scope

This Technical Report for Rel-5 identifies and describes enhanced user privacy in location services (LCS) and the corresponding functional requirements. The TR describes some possible enhancements to the privacy mechanisms provided for Location Services to support the increasing number of LCS clients and the varying privacy requirements for location services. The TR describes the stage-2 type of functional requirements for enhancing user privacy in location services that may be moved to the LCS Stage 2 specification TS 23.271, as seen feasible by TSG SA2.

The basic network solution as standardized in TS 23.271 Release 5 is described in general terms in the TR, with an indication of what enhanced privacy features are supported in Rel-5. The further enhanced LCS privacy features in Rel-6 and some alternative network solutions to support user privacy in Release 6 are also described and compared.

It should be noted that the GMLC-GMLC interface (Rel-6) is not taken into account in most network alternatives described in this report.

This TR defines the enhanced support of user privacy in location services regarding:

- General description of enhanced user privacy in location services
- Definition of enhanced user privacy in location services capabilities
- Functional requirements ~~Charging aspects~~
- Security aspects
- Roaming, service availability and continuity
- Relation between privacy issues in Presence and Location services.

2. References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document in the same Release as the present document.

[1] 3GPP TS 22.071

[2] 3GPP TS 23.271

3. Definitions, symbols and abbreviations

3.1 Definitions

Codeword: Target Subscriber defined access code, which must be provided by requestor in order not to get the location request rejected. The codeword is privacy information.

Privacy profile register (PPR): a functional entity containing a database with subscriber privacy information for location services and functionality to perform the related privacy checks. Note: the PPR is used in the architectural alternatives described in sect. 7.1 and 7.2.

Requestor: the originating entity, which has requested the location of the target UE from the LCS client.

Requestor Identity: This identifier is identifying the Requestor and can be e.g. MSISDN or logical name.

Service Type: The LCS Server maps the services indicated by an LCS Client into a Service Type as specified in TS 22.071.

Service Identity: Identity of the service under certain LCS Clients

User: The subscriber and user of the target UE

3.2 Abbreviations

PPR Privacy Profile Register

4. General description

In current Specifications only limited screening for privacy is possible. The screening is based on the "LCS client ID" parameter of MAP Provide Subscribe Location message used by GMLC to request the subscriber's location from SGSN or MSC. The visited MSC or SGSN maps the received LCS client ID to subscriber's Privacy parameters (e.g. list of allowed LCS clients) to screen out the unwelcome location requests. In practise, there is a need to have more detailed service type screening e.g. to differentiate between "where am I" type of services and games or entertainment services.

Additionally, it will be difficult for a subscriber to use local location based services when roaming. The subscriber does not have proper means to add local LCS clients to the allowed LCS client list in the Home environment HLR. Furthermore, the privacy parameters are defined with quite a narrow scope in the HLR, which may make it difficult for the subscriber to set additional and varying privacy parameters per LCS client.

According to the current specifications, the subscriber cannot receive any information regarding who originally asked for the location of the subscriber. Subscribers should be notified about the Requestor identity and it should be possible to allow the location information to be given only to those requestors, who are entitled to have it. All subscribers' location information should anyhow be protected against unwelcome location requests.

In order to protect the UE against the unwelcome location requests, the LCS shall support the screening function which denies the unwelcome accesses to UE The current LCS specification only supports the screening mechanism using the external identity of the LCS client and there is a need to enhance the screening mechanism e.g. using "Allowed Requestor List" or "Codeword".

5. Functional Description and Functional Requirements

5.1 Service Type Privacy

The user may wish to differentiate between privacy requirements even with one LCS Client, depending on which service the user requests from this LCS client or which service the LCS client offers to the user.

The LCS client requests location information for a target UE from GMLC. Currently the location request contains at least~~only~~ the identity of the LCS client and the identity of the target UE. The LCS client request is screened by GMLC using the identity of the LCS client. The screening mechanism is enough for the basic type of location requests, but

there is a need to enhance the functionality of the mechanism because one single LCS client may offer or support several or a multitude of different services. It is clear that the target UE user will have different privacy demands for different services, even when only one LCS client offers the services.

The enhanced mechanism should enable the users to allow their location information to be given to all LCS clients providing an indicated type of service. The user could e.g. allow all dating type services to get location information. The location request message issued by the LCS client to GMLC may ~~could be enhanced to~~ include a service identity, which can~~would then~~ be interpreted by GMLC to indicate what services belong to a certain Service Type category. The subscriber should be able to define and set privacy rules based on service type, so that services under that service type can be handled according to the corresponding service type privacy setting.

The service requirements for service type privacy and the standardized service types are specified in TS 22.071 [1]. The service type functionality will~~would~~ allow subscribers to use location services more easily while roaming.
The service type could be seen as an attribute of the LCS client and the LCS client name could contain the service type. ~~The service type shall be defined in a useful way and i~~It shall be possible to verify that the service identity~~type~~ indicated by the LCS client is correct.

~~Note: There are opposite views regarding whether the service type check may be done in the network or only by the target user~~

Service type checking by the target would be a "looser" way of defining services, and allowing users and client more freedom in defining services, while service type checking by the network would require some standardization, but would allow the network to control "spamming" towards the target.

~~Service type checking on application level avoids unnecessary signaling in core network, i.e. filters out the Location requests that anyway are going to be rejected.~~
~~In addition~~ It is noted that application/content providers probably could support ~~can start offering (if not already done?) this kind of~~ proprietary application based service identity privacy without waiting for Rel-5 of 3GPP.

It is emphasized that the service types offered by a certain LCS Client is to be part of the LCS Client service profile, which shall be known by the GMLC. An LCS client is hence not able to claim to offer services that are not included in its profile. The service type should ~~can also~~ only be conveyed between PLMNs with valid roaming agreements.

The LCS Server (PLMN) shall map the service identity given by the LCS client to a service type. The operator defines to what service type the given service identity belongs to.

~~For the benefit of roaming users it is vital to~~ Rel-5 includes a standardized ~~a~~ set of service types that can be used globally in all PLMNs. It shall be possible for the network operator/service provider to define additional service types that need not be globally unique. It is foreseen that the defined service types will be further elaborated in SA1 and possibly new service types added in Rel-6.

5.2 Support for enhanced privacy checking

It is seen that the current way to handle the privacy related settings in the network is probably too limited to support the increasing number of LCS clients and the varying privacy requirements for location services. It should also be possible for the user to set or change the location related privacy parameters in the home environment. SA1 has decided that Release 6 should include new flexible ways to set privacy requirements, e.g. according to time, day of week and user location. In order to support such additional privacy settings for location services architectural changes may be needed, see chapter 7. Regarding privacy settings based on time of day, the time of the visited network could apply or e.g. some universal time, like UTC, but this is for further study.

For compatibility reasons to pre-Rel-~~6~~4 the MSC/SGSN and HLR privacy functionality has to be kept regarding call/session related class, ~~(~~notification and ~~/~~verification of the location request~~)~~.

The enhanced network support for flexible privacy settings, e.g. based on location, time of day, etc., is not included in the scope of Release 5.

5.3 Requestor

In the current 3GPP LCS specifications only the LCS client is identified and authorized when a location based application is requesting the position of a target UE and in the original LCS specifications the LCS client itself was the originator, i.e. requestor, of the location information. The GMLC may store an "Authorized UE List", which holds MSISDNs or groups of MSISDN of the target mobiles, for which the LCS Client may issue a location request [2].

Within 3GPP scope there is no mechanism for the target UE user to activate a certain application with a known LCS client, but still be able to restrict who are allowed to get position information regarding the target UE. A simple example of this type of service is a "Friends finder" application. Currently there is only a relation between the LCS client and the MSISDNs it is allowed to issue location request for, but there is no relation between the originating requestor and the target UE. This prevents the target UE user from authorizing the originating requestor.

~~Note 1: It is FFS if the relation between the originating requestor and the target UE could be handled by the application. Applications like the "Friends finder" typically already today provide this kind of relation.~~

TS 22.071 [1] specifies a new service requirement in Rel-5, that the Location Request issued by the LCS client should be enhanced to optionally include also the identity of the originator of the location request, i.e. the Requestor, not only the identity of the LCS client. The scenario is developed such, that the requestor is connected to the LCS client as a separate entity, with its own identity. Because of this, also the requestor shouldmust be authenticated by the LCS client ~~and/or the network~~.

~~Note 2: Other security aspects of the Requestor functionality should be further studied.~~

Note ~~3~~: It is seen that when the requestors are authenticated by the LCS client, the LCS client should not use the same requestor identity for several requestors.; Wwhen the requestors are authenticated by GMLC the GMLC should not use the same requestor identity for several requestors. On the other hand, the requestor identity could be used to~~the~~ identifty ~~of~~ a ~~closed~~ user group that could be used by and for different requestors, but this is for further study.

The identity of the Requestor shall be included in the privacy interrogation request, when this is sent to the target UE and shown to the user.

The basic requestor functionality is included in Rel-5 and may be further enhanced in Rel-6, see chapter 8.

~~This functionality should possibly be introduced already in Rel-5.~~

5.4 User Control

The target user must have full control regarding who can get his or her location information. The LCS stage 1 specification 22.071 [1] contains the following text on user control:

"The user shall be able to change the following settings in the privacy exception list.

- the LCS Client and/or group of LCS Clients list
- the target UE user notification setting (with/without notification)
- the default treatment, which is applicable in the absence of a response from the target UE for each LCS client identifiers"

In addition the user should also be able to change privacy settings for the service types, Requestors and Codewords in Rel-5 and the time and location based privacy settings in Rel-6. The mechanisms for user control are outside the scope of this Technical Report~~FFS~~.

5.5 Codeword

The codeword is an optional function for LCS location services to protect UE against third party monitoring his/her location.

The location request from the LCS client/Requestor may include the codeword for the target subscriber. The PLMN compares the codeword sent from the LCS client/requestor with the codeword, which is registered to the PLMN in

advance. If the comparison of the codeword is successful, then the location request is not rejected. If the comparison fails, the PLMN judges that the location request shall be rejected. After the codeword is checked and the check is successful, the privacy setting in the current specification will be checked. The privacy setting in the current specification is not overridden even if codeword check is successful. The codeword is registered in the PLMN by the subscriber. The subscriber may register multiple codewords. In this case, the location request is not rejected if the received codeword is included in the codeword list of the subscriber. The subscriber of the UE is responsible to distribute his/her codeword to such requestors, whom the subscriber has allowed to request his/her location. Once the codeword has been set and properly distributed, the subscriber is protected against the location request from a third party that does not know his codeword.

Optionally, the subscriber may specify that the codeword is not checked in the PLMN, but instead be passed to the subscriber as additional information to be used by the subscriber to determine whether or not the location request should be authorized.

The mechanism for distribution of the codeword to the requestors and registration of the codeword by the UE subscriber with the operator is outside the scope of 3GPP. The mechanisms to generate the codeword are not yet described in this Technical Report and it is for further study whether the mechanisms need to be standardized. The codeword is applicable to the value added services only.

The codeword may be checked by the user of the UE or by the network.

TS 22.071 [1] specifies the service requirements for the codeword function and the codeword functionality is part of Rel-5.

5.7 Anonymity

For enhanced privacy the subscriber's true identity (MSISDN) can be hidden and replaced with an alias that is used as a permanent or temporary reference of the subscriber, both when being a target and when being a requestor. ~~As one solution t~~The alias can be passed on from the terminal to the LCS Client application when the subscriber invokes a request e.g. to a specific service type. As another solution, ~~a~~some secured network proxy may allocate the anonymous ID (alias) to replace MSISDN. The LCS client will use alias as ~~an~~ identifiers for the target subscriber instead of using the true MSISDN identity. GMLC will ~~in response~~ use the same alias, when sending the response to the LCS client. It should be possible to define both permanent and temporary alias.

The service requirements for anonymity are to be discussed and agreed in SA1 and specified in TS 22.071 [1] for Rel-6.

5.8 Related privacy issues in Presence and Location services

Location information is an important part of the Presence information used in the Presence service. ~~The subscriber should be able to set privacy requirements also for the location information used in the Presence service. Preferably the privacy settings and control mechanisms that the subscriber has defined for location services should be applicable as such also for the location information in Presence services.~~

~~Privacy settings for presence could possibly be shared with LCS, but it need further discussion is needed between presence and LCS people.~~

~~The relations between privacy issues in presence and in LCS should be discussed in SA1 and SA3.~~

~~11. Common stage 2 privacy issues in Presence and Location services~~

The Presence service may act as ~~a~~ LCS client and request location information from GMLC. The target mobile user shall be able to define privacy rules for the Presence server, as being an LCS client. The location request and privacy are handled as specified in 23.271 for this LCS client.

The presence information (including location information) is used according to privacy settings as defined for the presence service.

If the watchers are trying to obtain the presence information including location information of the presentity via presence service the following three conditions have to be met:

1. The Presence service must be set up as an LCS Client in the Location services, so that the Presence service can get the location of the Presentity.
2. Presentity has to set the access rules to allow the particular watcher to see the presence information (including location).
3. Location services must be provisioned for the presentity and the Presence service has to be included in the subscriber's (presentity's) LCS Privacy Profile (SLPP). ~~The Presence service itself may request from the location server what are the privacy settings that shall be applied for the location information of the target mobile before forwarding location information or other presence attributes to other parties.~~

~~Possible differences between privacy settings in presence and in LCS should be resolved.~~

5.9 Summary of enhanced user privacy in location services in Rel-5 and Rel-6

Table 5.1 summarizes the enhanced user privacy features in Release 5 and Release 6.

Table 5.1: Enhanced user privacy features in Release 5 and Release 6.

Feature	In Release 5	In Release 6	Comment
Service Type Privacy (5.1)	Yes	Yes	may need to be further elaborated for Rel-6
Flexible privacy settings (5.2)	No	To be developed for Rel-6	
Requestor (5.3, 8)	Yes	Yes	may be enhanced in Rel-6, see chapter 8
Codeword (5.5)	Yes	Yes	may need to be further elaborated for Rel-6
Anonymous target and anonymous requestor (5.7)	No	To be developed for Rel-6	

There may be differences in the network support for enhanced user privacy in Rel-5 and in Rel-6. The Rel-6 solutions should be developed taking in account interworking with pre-Rel-6 releases.

6. Network support for user privacy in Rel-5 ~~Stage 2 description of service type privacy~~

The service requirements for several enhanced user privacy features have been specified for Rel-5 and these features are supported by the network in Rel-5 as listed in chapter 5.9. The Rel-5 enhanced privacy features are shortly described in this TR for comparison reasons, but the corresponding LCS specifications contain the complete documentation of the supported features, see TS23.271.

6.1. Network support for Service Type and Codeword in Rel-5

LIF has defined a 'Service Identity' information element, which is used to identify the services offered by the LCS client. The LCS client shall forward the service identity information in the LCS Service Request on the Le interface

~~from the LCS client~~ to the GMLC. ~~It is for further study whether t~~The GMLC ~~or PPR (privacy profile register)~~ shall map the received service identity to a specific Service Type when the service is provisioned in GMLC. The supported Service Types in Rel-5 are specified in TS22.071. If GMLC only receives the LCS client identity but not the service identity, the GMLC may report an error to the LCS client, or in case the LCS Client is explicitly so authorized, proceed with the request. The service type information may be included in HLR/HSS ~~and in the Privacy Profile Register~~. Also the Provide Subscriber Location MAP message sent by GMLC on the Lg interface to MSC and SGSN may contain the Service Type information.

In order to support the service requirements for service type and codeword in Rel-5, the LCS architecture as specified in LCS stage 2, TS 23.271 Rel-4 is used, without any addition of new nodes/network entities.
~~The service type can be defined in a similar way as Annex C in TS 22.071, which describes the attributes for specific services.~~

~~The service type privacy setting could be the same as the 5 privacy settings listed in Annex A of 23.271, but in addition it may be necessary to define some new privacy settings according to service type.~~

6.2 Network support for Requestors in Rel-5

TS 22.071 [1] specifies a new service requirement in Rel-5, that the Location Request issued by the LCS client should be enhanced to optionally include also the identity of the originator of the location request, i.e. the requestor, not only the identity of the LCS client. In Rel-5, if the LCS client provides a requestor identity, the GMLC shall send it as separate information. In addition, in order to display the requestor identity in case of pre rel-5 network elements (i.e. MSC and/or UE), the requestor identity may be also added to the LCS client name by GMLC (this is supported in Rel-5). The requestor indication is further described in chapter 8.

~~6.1 Privacy profile register (PPR)~~

~~The PPR as used in the architectural alternatives of clause 7.1 and 7.2, contains a database with the subcribers privacy information and performs the related privacy checks and reports the result to the requesting entity.~~

~~It is FFS and dependent on the architectural alternative, if the PPR should also be used for mapping of the service identities exchanged between LCS client and GMLC to service types used for roaming scenarios.~~

~~It is FFS, if the PPR should be used for interoperations between LCS and other services, e.g. presence service.~~

7. Network support for ~~Stage 2 description of~~ enhanced privacy checking in Release 6

LCS Stage 2 specification TS 23.271 defines only a limited set of privacy options in chapter 9.5.3 consisting mainly of five different privacy settings:

- positioning not allowed;
- positioning allowed without notifying the UE user (default case);
- positioning allowed with notification to the UE user;
- positioning requires notification and verification by the UE user; positioning is allowed only if granted by the UE user or if there is no response to the notification;
- positioning requires notification and verification by the UE user; positioning is allowed only if granted by the UE user.

These settings in the network are probably too limited to support the increasing number of LCS clients and the varying privacy requirements for location services especially for roaming subscribers.

It should be possible to have variable privacy settings, e.g. according to time of day, day of week and according to the location of the target UE. However, for compatibility reasons to Rel-4 the MSC/SGSN and HLR privacy functionality has to be kept to support (notification and/ verification).

Note 1: It is FFS if these additional privacy settings could be handled by the User Profile services as specified in 3GPP.

In order to keep the compatibility with pre-Rel-64 privacy functionality (notification/verification), the concept of "pseudo-external identity" is used in Rel-6 and later releases~~introduced~~. In the current stage 2 specification 23.271, the external identity is defined as the identity of external LCS client. The pseudo-external identity is not the identity of real external LCS client but the identity, which is used for notifying SGSN/MSC of the location request class (call/session related or non-related) and the required type of indication for the target UE user. The pseudo-external identity shall be defined by each operator. Eight pseudo-external identities shall be defined according to the type of indication and the location request class (call/session related class or not). The eight pseudo-external identities are summarized in the table 1. Operator allocates E.164 addresses for the pseudo-external identities.

Table 1: Pseudo-external identities

Pseudo-external identity	Llocation request class	Ttype of indication
Pseudo-external identity 1	Call/Session related class	Location allowed without notification
Pseudo-external identity 2		Location allowed with notification
Pseudo-external identity 3		Location with notification and privacy verification; location allowed if no response
Pseudo-external identity 4		Location with notification and privacy verification; location restricted if no response
Pseudo-external identity 5	Call/Session non-related class	Location allowed without notification
Pseudo-external identity 6		Location allowed with notification
Pseudo-external identity 7		Location with notification and privacy verification; location allowed if no response
Pseudo-external identity 8		Location with notification and privacy verification; location restricted if no response

Note: More pseudo identities may be required.

The pseudo-external identities are registered in HLR/HSS as SLPP of each UE in advance.

When a GMLC receives a location request, the GMLC performs the privacy check, may-be with PPR. In case negative result of the privacy check, the GMLC immediately returns the response back. In case positive result, in order to indicate SGSN/MSC which type of indication (notification/verification) is required for the location request, the GMLC selects a proper pseudo-external identity according to the privacy check result. Then the GMLC replaces the external identity to the selected pseudo-external identity. The original external identity may be included in the LCS client name field if the operator want to notify the UE of not only original LCS client name but also the original identity. Then the GMLC sends Provide Subscriber Location message to MSC/SGSN as specified in 23.271. The SGSN/MSC selects the type of behavior according to the SLPP of the target UE and the pseudo external identity.

With the pseudo-external identity, it is possible to enable the Rel-4 MSC/SGSN to behave according to the result of the enhanced privacy check mechanism without any modification of the Rel-4 SGSN/MSC. The pseudo-external identity also enables to handle the call/session related class.

Even in the case when the target UE wants to be protected by the enhanced privacy check mechanism and the original external identity is replaced by the pseudo-external identity, the target UE can receive the client name of the LCS client to identify the LCS client. In the case when the target UE does not want to be protected by the enhanced privacy check mechanism and the HSS stores the SLPP including the original external identity list, the original external identity is sent to the target UE as previous release.

Even with the pseudo-external identities shown above, the enhanced privacy parameters (i.e. Requestor ID, Codeword and Service Type) cannot be notified to the target UE, when the SGSN/MSC is Rel-4.

It should be noted that the network nodes and interfaces in the alternative network solutions described below may use the same name e.g. for different interfaces.

7.1 Architecture alternative with privacy profile register (PPR)

7.1.1 Architecture

In order to support additional privacy settings for location services the HLR/HSS may indicate that the subscriber's additional privacy information for location services is available in an external database, e.g. the Privacy Profile Register (PPR). The PPR may contain additional privacy settings, e.g. according to time of day, day of week and according to the location of the target UE. In case the PPR have executed the additional privacy check and given the result back to GMLC, then GMLC will in case of positive result from PPR forward the Location Request to MSC/SGSN as specified in 23.271 or in case of negative result from PPR immediately return the response back to LCS Client. The PPR is accessible from the GMLC via the Lr interface. This is illustrated in figure 7.1.

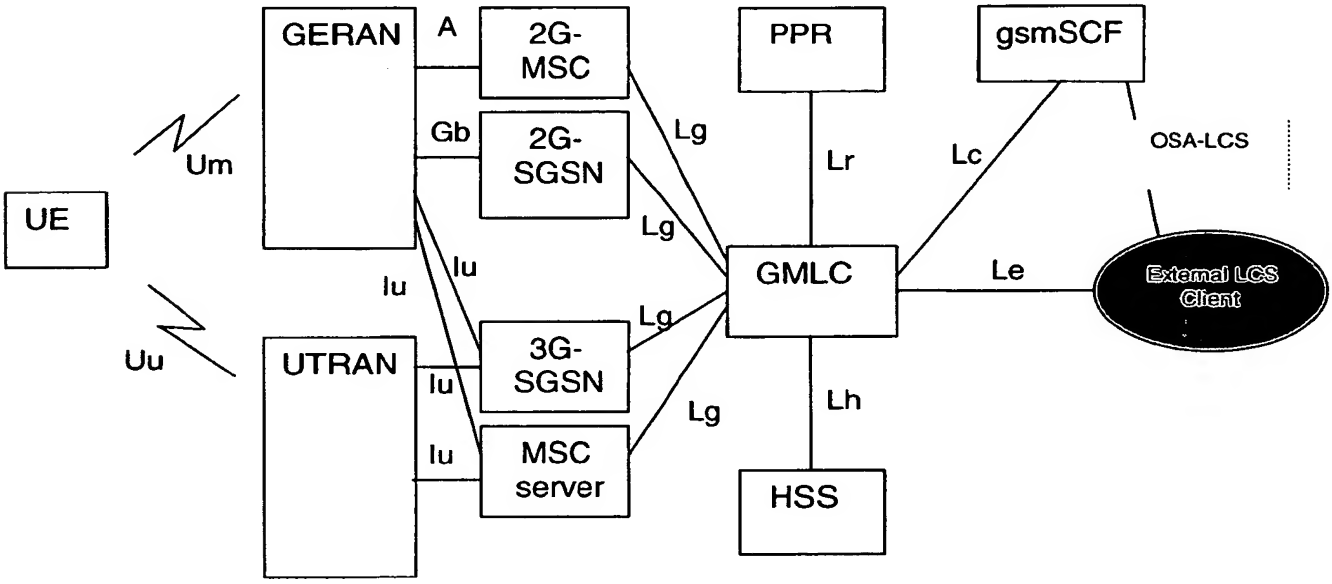

Figure 7.1.1; LCS architecture alternative with PPR attached to GMLC

The PPR is normally managed by the PLMN operator and there is trusted signaling between GMLC and PPR. When the request has to be delivered via an unsecured network, (e.g. the public IP-network) the PPR server needs to be authenticated and the traffic has to be secured.

The PPR could be located outside the operator's core network, but this type of architecture is outside the scope of 3GPP.

Privacy check according to Rel-4 and Rel-5 (privacy check in MSC/SGSN) and the additional "privacy check" of GMLC/PPR (as described in this TR) may lead to different results

GMLC sends the privacy check request to PPR. If the privacy check was approved by the PPR it will report to GMLC whether the subscriber wants to be notified, verified or whether the request is allowed without notification. GMLC will use this result and pass it on to the MSC/SGSN as an additional "result" field in the PSL message on the Lg interface. There are 3 alternatives how to combine the PPR result with the privacy checking in MSC (Rel-~~6~~5):

1. MSC shall check as specified in TS 23.271, whether the subscriber has blocked all LCS services, in which case the PPR result shall be rejected. In all other cases the PPR result shall be used as described in alternative 3 below, see note 3.

2. MSC shall also perform a privacy check as specified in TS 23.271, Rel-4 or Rel-5 as applicable, in the following cases:
   - PPR result is not received or MSC does not understand the result.
   - PPR result is received but not used.

3. MSC receives the PPR result and shall start MT-LR according to the result, see note 3.

All the alternatives are configurable result handling routines. MSC can be configured so that one of alternatives 1, 2 or 3 is defined as default routine for each GMLC that is allowed to request for location from this MSC. MSC verifies what GMLCs are allowed to do location as defined in TS 23.271. The HLR sends the PPR address per subscriber in the SRI response to GMLC and when a PPR is indicated, the GMLC may select that the privacy check is to be performed in the PPR pointed out by HLR. The Home PLMN operator is able to define what is the physical address of the logical entity PPR. The operator may even allow the subscriber to specify the location of the PPR and define the corresponding PPR address in the HLR/HSS
This solution is especially feasible in roaming situations, since the PPR address is received from the HLR/HSS and the privacy is always checked in a single point that holds the subscriber's privacy rules.

With this architecture alternative, when the PPR holds all the subscribers privacy information and if the privacy check fails the location request can be rejected already at that point. This means that there is no need to send the location request further to MSC/SGSN This functionality hence reduces the MSC/SGSN and the Lg interface capacity load.

The privacy settings in HLR and PPR shall be consistent with the privacy settings in PPR, but this is seen as a network management issue outside the scope of this TR.
If the GMLC supports this enhanced privacy check functionality including the Lr interface it should inform HLR about this in the SRI procedure. If HLR does not receive such information -it can anticipate that the enhanced privacy check could not be handled. HLR can in this case select to reject the location request if necessary or send routing information to GMLC.

Note 1: SA3 will investigate~~be asked to verify~~ whether the preferred solution alternative is acceptable from security point of view.

Note 2: It should be defined in MSC/SGSN what is the level of trust that MSC/SGSN can apply for the privacy setting result sent by GMLC/PPR, also when GMLC is in another country. This can be done using result handling routines 1 and 2, as described above.

Note 3: GMLC includes in the privacy request to PPR an indication whether the Location request is call/session related or not.

Note 4: In case of deferred MT-LR, ~~it is FFS if the MSC should ask via the GMLC to ask the PPR to make the privacy check again, because the subscriber may have changed the LCS privacy information during the time when the target mobile was not available~~PPR will notify GMLC to make a new privacy request for the corresponding target mobile, if the user has changed privacy settings and there exists ongoing location request at the moment.

7.1.2 Information Flow

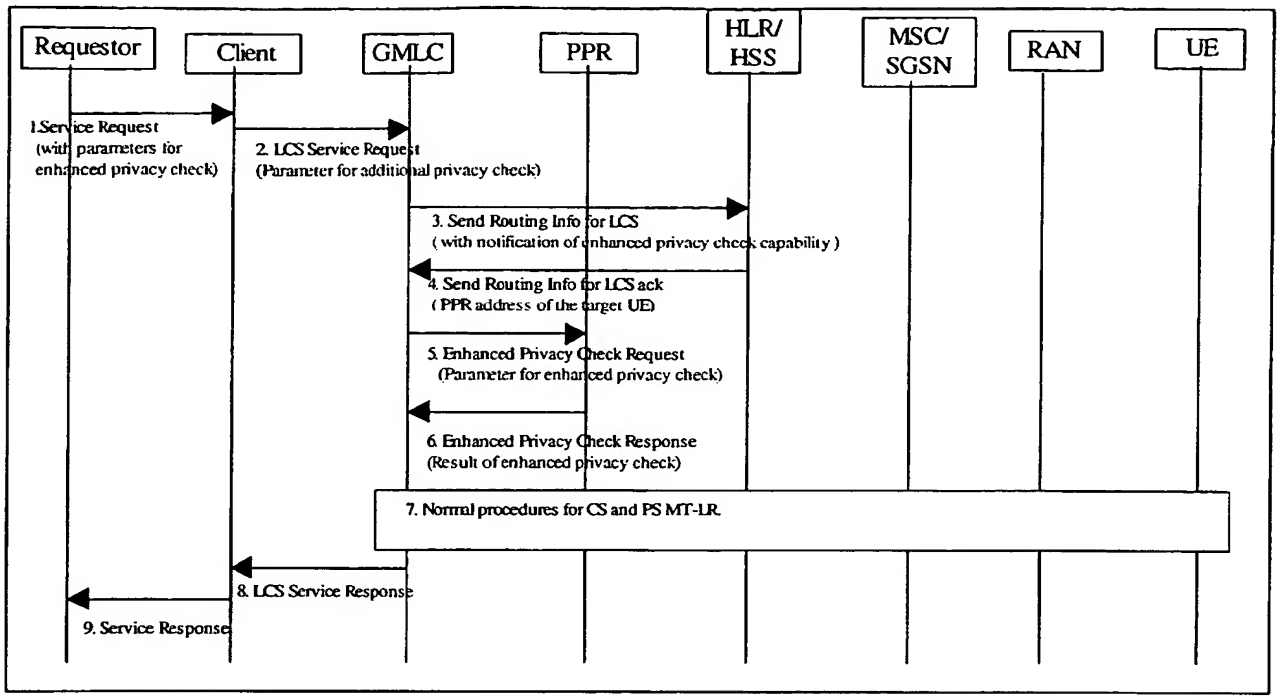

Figure 7.1.2; General information flow for the architectural alternative with the PPR attached to GMLC

*Note 1. The Enhanced Privacy Check Request may contain the codeword and the service type.

*Note 2. The Requestor ID and the codeword shall be sent to the MSC/SGSN if they are wanted to be shown to the UE user in the LCS notification invoke procedure. Also the privacy check result shall be carried to the MSC/SGSN.

7.2. Architecture alternative with privacy profile register (PPR) attached to MSC/SGSN

7.2.1 Architecture

In order to support additional privacy settings for location services the HLR/HSS may indicate that the subscriber's additional privacy information for location services is available in an external database, e.g. the Privacy Profile Register (PPR). To support these additional privacy settings (e.g. settings concerning service type, requestor ID etc.) in case of national and international roaming, the PPR is accessible from the MSC/SGSN via Ld interface.

The privacy checks according Rel-4 privacy settings remain in the MSC/SGSN, the classification of the location request - call related/unrelated, PLMN operator - as well as the overall control of privacy checks - notification, verification, (emergency), privacy override - may be still located in the MSC/SGSN. In case the PPR has executed the additional privacy check and given the result back to the MSC/SGSN, the MSC/SGSN may decide – possibly dependent on information about whether the UE is in its home PLMN or it is roaming – how the result of Rel-4 or Rel-5 checks and the result of the additional privacy checks have to be merged (decision concerning verification/notification etc.).

The address information of the referring PPR is stored in the privacy data of the subscriber in the HLR/HSS. In this way the PPR is known to the (visited) MSC/SGSN in case of national or international roaming. The PPR contains all privacy data or - for Rel-4 compatibility reasons - only the additional privacy settings. The PPR may contain only data of subscribers belonging to that PLMN.

For synchronization purpose between PPR and HSS/HLR concerning possible common privacy data the PPR may be connected to HLR/HSS via Lt interface. This interface may also be used for change of privacy settings e.g. by means of a SCI procedure through HLR/HSS.

Determination of a call or a session to a LCS client to which the UE has an active connection is done in the MSC or SGSN respectively. This information will be applied for the call/session related privacy checks in the SLPP of Rel-4, Rel-5 and the Rel-~~6~~5 enhancements in PPR accordingly.

The notification and verification settings for the enhanced privacy check in the PPR are reported as result to MSC/SGSN, where the according procedures towards the UE are initialized.

Note 1: With this architecture enhanced privacy checking in case of national and international roaming is possible.

Note 2: The Rel-4 and Rel-5 compatibility is given within this architectural proposal.

Note 2: As requested by the WI (SP-010574) this architecture allows the user easily to set or change the location related privacy parameters in the home network / PPR.

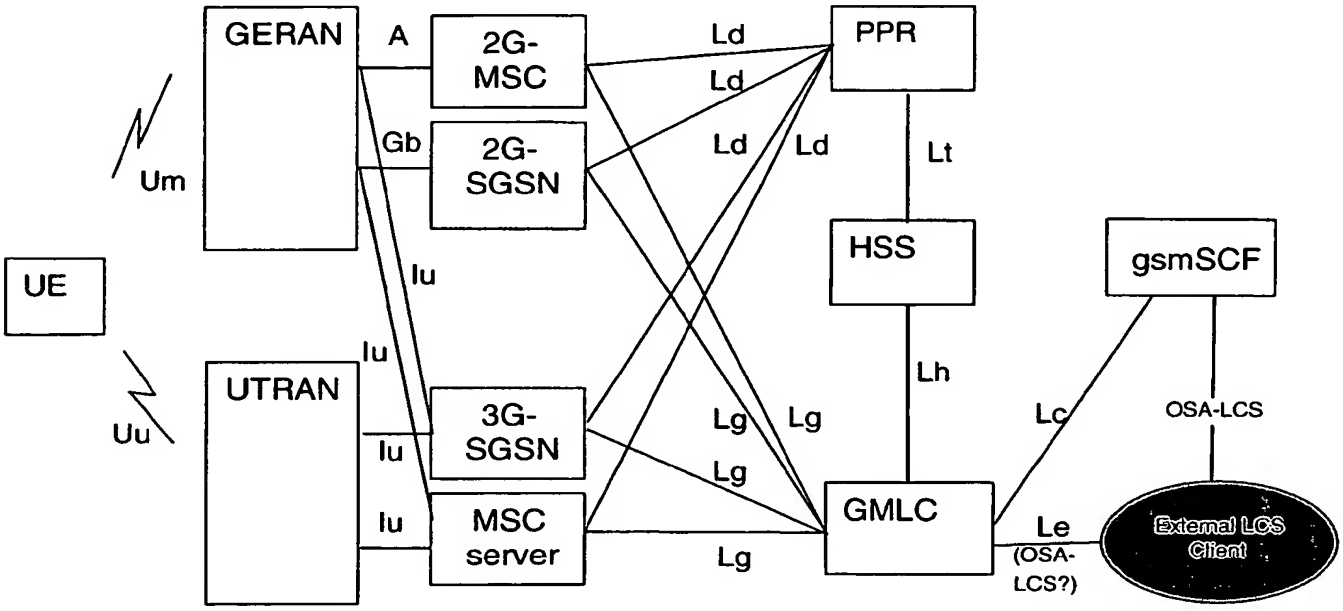

Figure 7.2.1; LCS architecture alternative with PPR attached to MSC/SGSN

7.2.2 Information Flow

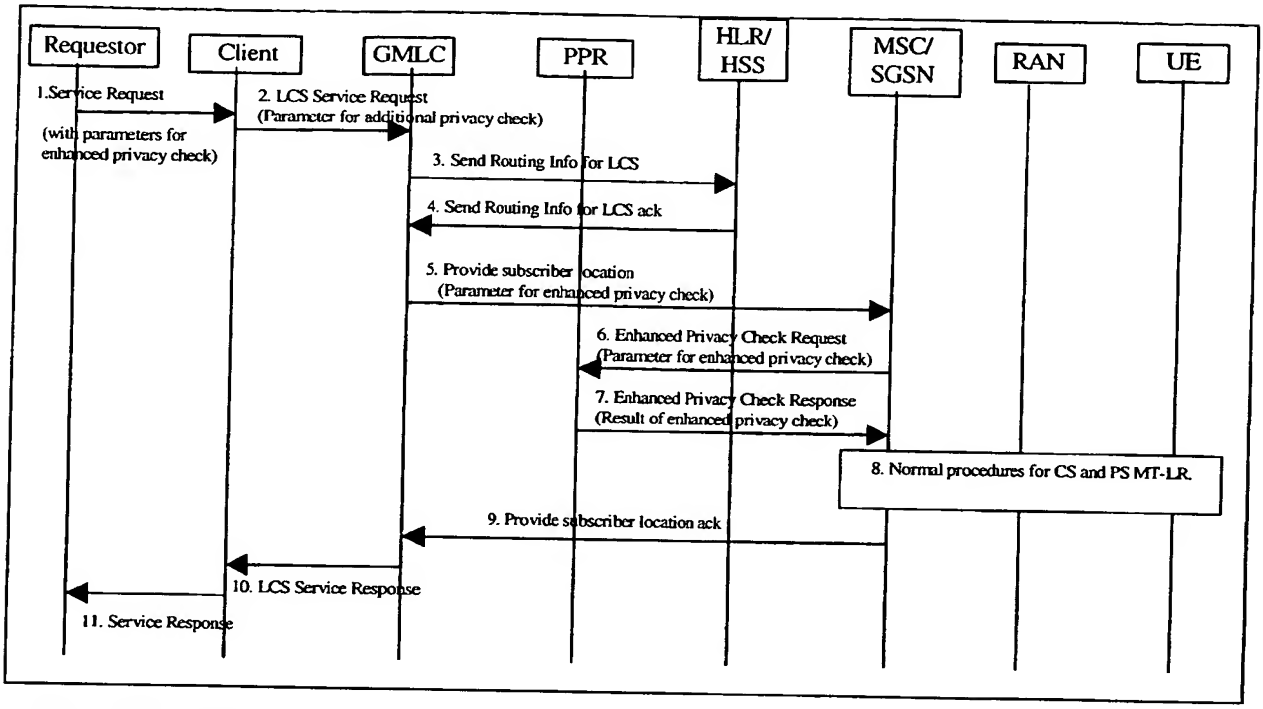

Figure 7.2.2; General information flow for the architectural alternative with the PPR attached to MSC/SGSN

7.2.3 Exceptional handling

The privacy settings for an active deferred MT-LR may have been changed while waiting for the event: For this, the MSC/SGSN shall access the PPR again, when the event is detected.

7.3. Architecture alternative with Home GMLC

7.3.1 Architecture

In order to support the enhanced privacy settings for location services the HLR/HSS may indicate that the subscribers' additional privacy information for location services is available in a particular GMLC, i.e. Home GMLC of the subscriber. The Home GMLC may contain additional privacy settings of the subscriber, e.g. according to time of day, day of week and according to the location of the target UE. The HLR/HSS sends the Home GMLC address per subscriber in the SRI response. The Home PLMN operator defines what is the physical address of the logical entity Home GMLC. In case a GMLC, (originated GMLC), which receives a location request from an external LCS client received the Home GMLC address of the target UE from the HLR/HSS and the address is not the same as its own address, the originated GMLC forwards the location request received from the external LCS client to the Home GMLC via Lr interface. Then the Home GMLC performs the enhanced privacy check. In case positive result the Home GMLC selects a proper pseudo-external identity, according to the required type of indication and the LCS privacy class (call/session related class or non-related class) of the location request, and replaces the external identity to the appropriate pseudo-external identity. Then the Home GMLC sends Provide Subscriber Location message to MSC/SGSN as specified in 23.271. If the target UE user's privacy setting does not require the enhanced privacy check and the HSS stores the SLPP including the original external identity list, the Home GMLC does not replace the external identity and sends Provide Subscriber Location message with the original external identity. The Home GMLC forwards the location report received from the SGSN/MSC to the originated GMLC. In case negative result of the enhanced

privacy check, the Home GMLC immediately returns the response back to the originated GMLC. The Home GMLC communicates with other GMLCs via the Lr interface. This architecture is illustrated in figure 7.3.

If a GMLC supports the enhanced privacy check functionality including Lr interface, it should send that information to HLR in SRI procedure. If that information is not received the home operator can then know that the enhanced privacy check could not be handled and the location request could be rejected already by the HLR.

With this architecture alternative, the Home GMLC holds the subscribers privacy information and if the privacy check fails the location request can be rejected already at the Home GMLC. That would mean that there is no need to send the location request further to MSC/SGSN. This functionality would reduce the MSC/SGSN and the Lg interface capacity.

When the Home GMLC concept is introduced, the deferred MT-LR is handled as following steps.

Step 1: When any privacy setting of a UE, which is held in Home GMLC of the UE, is changed, the Home GMLC checks whether there is any deferred MT-LR process related to the UE that the Home GMLC is waiting the event occurrence.

Step 2: If there is a deferred MT-LR process, where the GMLC is waiting for the event to occur, the Home GMLC checks whether it is necessary to cancel the deferred location process in SGSN/MSC.

Step 3: In case it is necessary to cancel the deferred location request the Home GMLC sends Provide Subscriber Location message to the SGSN/MSC in order to cancel the deferred location request process and returns response back to the original GMLC.

This solution is especially feasible in roaming situations, since the Home GMLC address is received from the HLR/HSS and the enhanced privacy check is always done in a single point that holds the subscribers' enhanced privacy settings.

The Home GMLC may hold both of the enhanced privacy settings and Rel-4 and Rel-5 privacy setting~~.~~. Rel-4 and Rel-5 privacy checks in SGSN/MSC are~~is~~ performed as in the previous releases in order to decide the type of indication for the target UE.

Note 1: The Home GMLC could not identify whether the location request is related to the ongoing call/session because the Home GMLC does not know about the called party number or APN of the ongoing call/session. The call/session related class shall be handled at SGSN/MSC as same as the current specification.

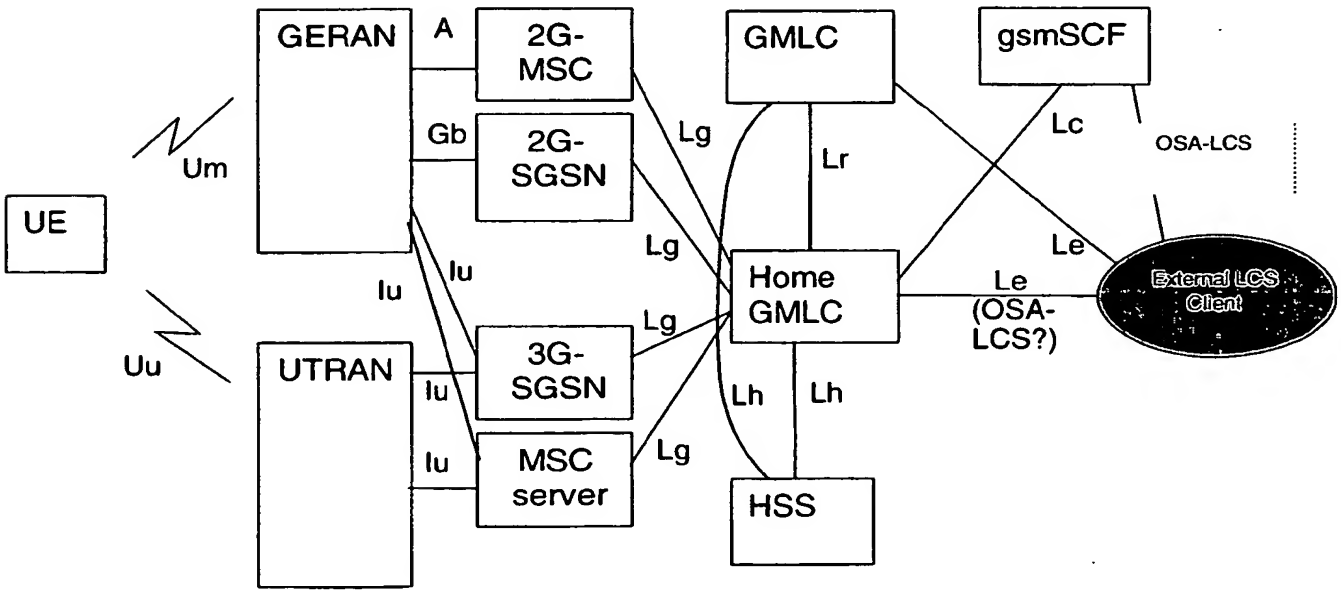

Figure 7.3.1; LCS architecture alternative with Home GMLC

Note 2: It may be necessary to ensure that there is no inconsistency between privacy settings in HSS and Home GMLC, when the Home GMLC will hold both the enhanced privacy settings and the legacy privacy settings. The synchronization of the privacy settings between Home GMLC and HSS could be realized by using O&M functionality or by using enhanced Lh interface. This is FFS.

7.3.2 Information Flow

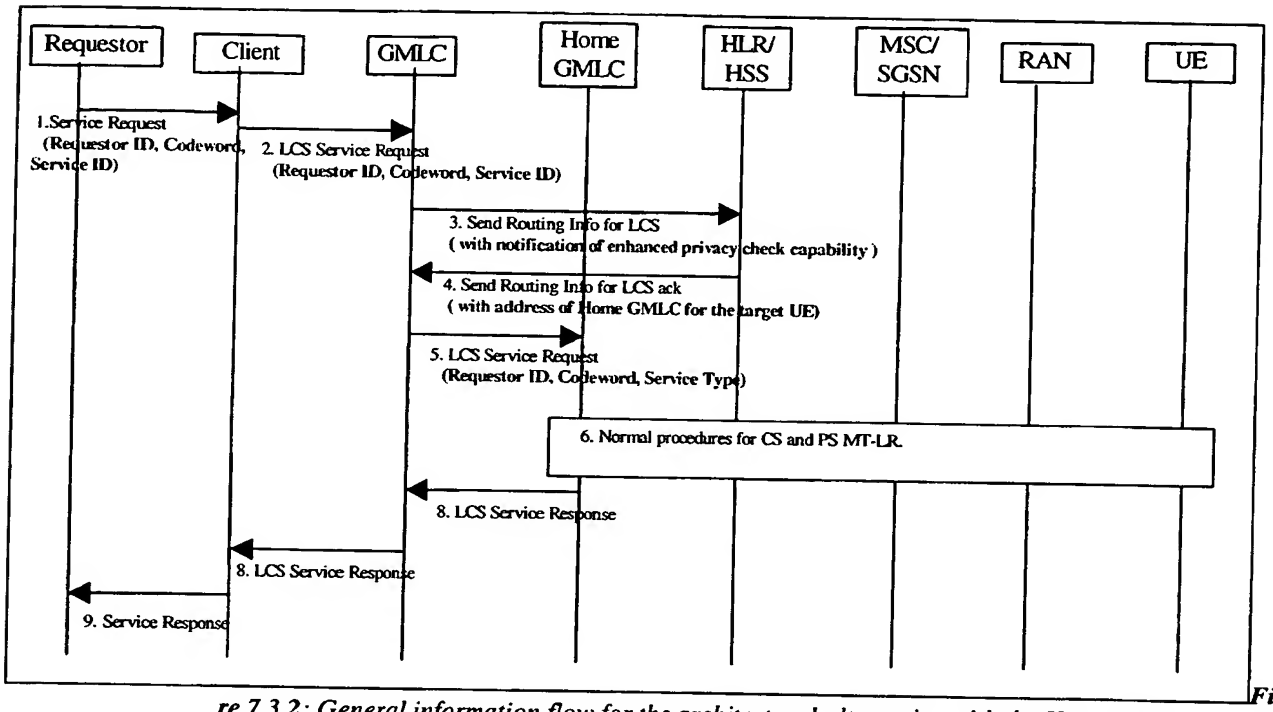

Figure 7.3.2; General information flow for the architectural alternative with the Home GMLC

Note : In step 6, the Requestor ID and the codeword shall be sent to the MSC/SGSN (Rel-5 and Rel-6) if they are wanted to be shown to the UE user in the LCS notification invoke procedure. Also the result shall be carried to the SGSN/MSC (Rel-5 and Rel-6).

The Home GMLC may in step 6 send also a pseudo-LCS client identity to MSC/SGSN of Rel-4 or earlier. This signaling step should be further detailed.

7.4 Architecture alternative with PPR associated with the HSS only

Section 7.4 was removed as other architectural alternatives consider similar mechanisms to what it introduced. This was done with the aim to simplifying the consideration and decision of the alternative methods.

~~7.5 Enhanced User Privacy using existing LCS architecture.~~

~~7.5.1 Architecture~~

~~In order to support the service requirements for enhanced privacy checks, the LCS architecture as specified in LCS stage 2 3GPP TS 23.271 rel-4 can be used, without the addition of new nodes/network entities.~~

7.5.2 Information flow

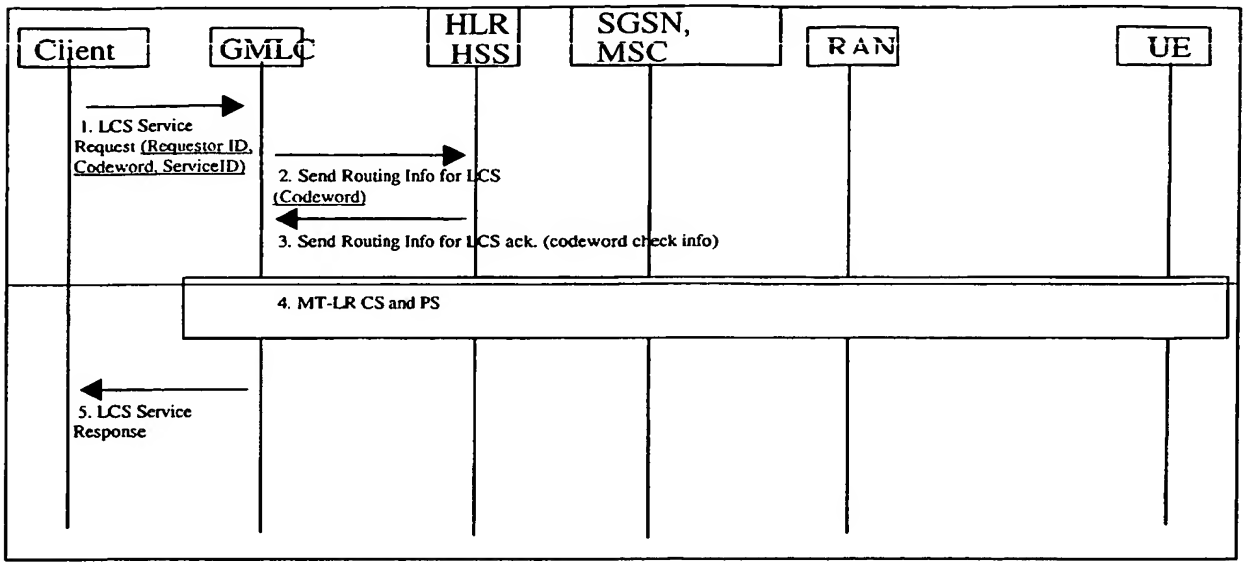

Figure 7.5.1; General information flow when using existing architecture

1. The LCS service request sent from the LCS Client to the GMLC carries the parameters for enhanced privacy checks (Requestor Id, Codeword and Service ID).

2. The GMLC verifies in the LCS client profile that the service ID received by the LCS client matches one of the allowed Service identities for that LCS client.

3. The GMLC sends a Send_Routing_Info_for_LCS message to the HLR/HSS, carrying the codeword received from the LCS client.

4. The HLR/HSS verifies that the Codeword received from the GMLC matches one of the codewords stored for the target subscriber. If the check is unsuccessful, the HLR/HSS sends an error indication to the GMLC and the LCS procedure is ended. If the check is successful, the HLR/HSS may verify that the VMSC supports the EUP mechanisms (this information is received in the HLR/HSS at location update in the "LCS supported capabilities set"). In order to protect the privacy of a roaming subscriber, the HLR/HSS may reject the Send_Routing_Info_for_LCS if the VMSC/SGSN does not supported enhanced privacy checks. If the codeword check is successful and the VMSC/SGSN supports the needed LCS capabilities, the HLR/HSS sends the VMSC/SGSN address in Send_Routing_Info_for_LCS_ack message.

5. If no codeword is registered in the HLR for the subscriber, the HLR shall not reject the request and inform the GMLC by setting the codeword check info in the Send_Routing_Info_for_LCS_ack message

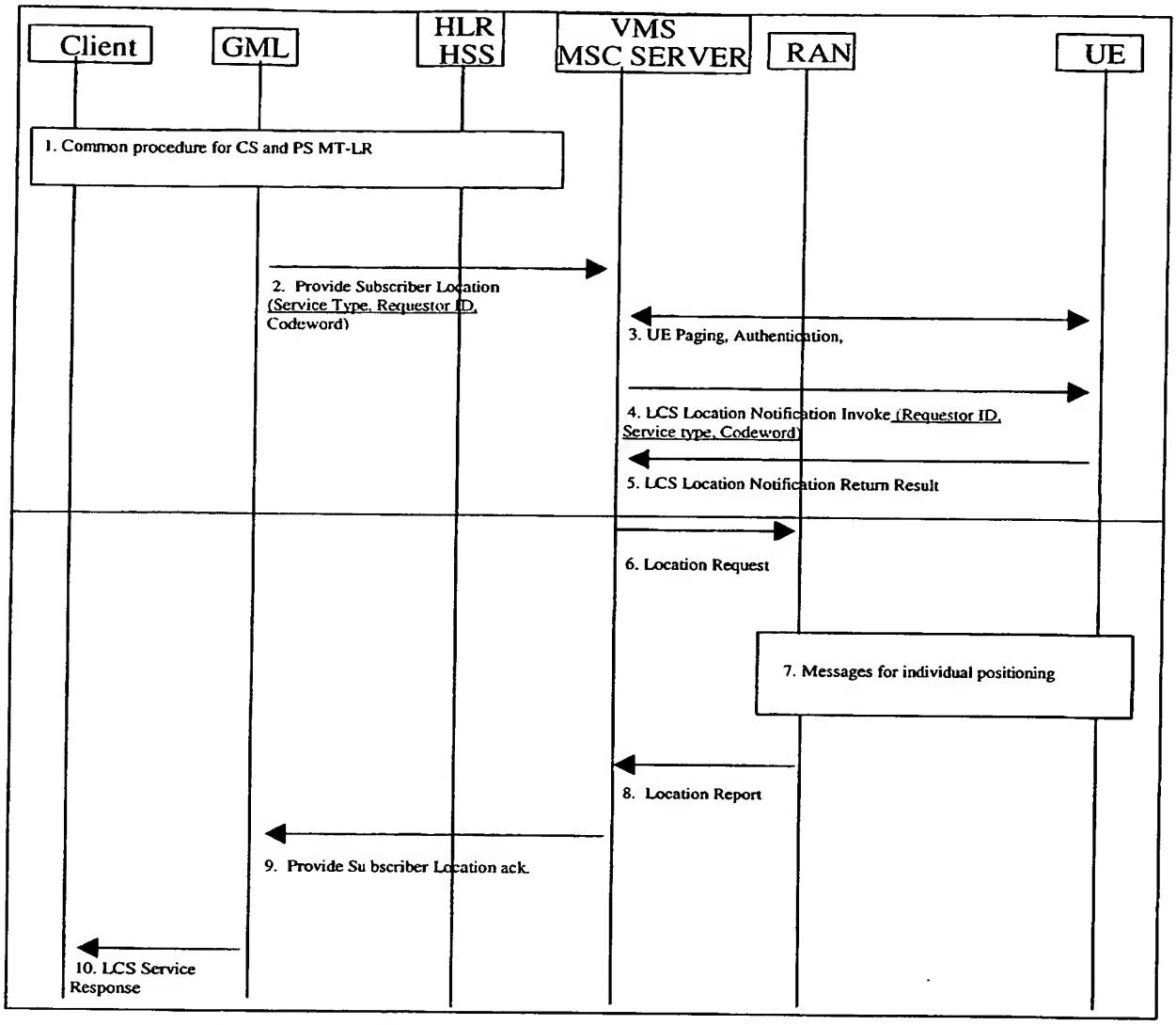

Figure 7.5.2; Continued general information flow when using existing architecture

6. The GMLC converts the service identity received by the LCS client in the proper service type and sends the service type and the Requestor identity in the MAP Provide Subscriber Location message. If the GMLC received the information that no codeword for the subscriber was stored in the HLR, the codeword shall be include in the Provide Subscriber Location message, in order to have the codeword check in the UE (note that the PSL message has to carry the codeword for notification, not depending of the chosen architecture).

7. If the SLPP contains service types/requestor ids, an CS-MT-LR/PS-MT-LR will be allowed by the MSC/MSC server or SGSN if the service type/requestor id supplied by the GMLC matches the identity of any service type/requestor id contained in the UE's SLPP. If the SLPP does not contain service types/requestor ids, the already existing privacy checks will be performed.

8. If notification has to be performed, the LCS Notification Invoke message will carry also the requestor ID, the service type and the codeword, if received.

7.6 5 Comparison between each architectural alternatives

Several architectural alternatives are proposed in Chapter 7. This section was set up for the comparison of network alternatives in Rel-5 and is not fully applicable for Rel-6 compares the proposed architectural alternatives.

Table 7.5.1; Comparison from operator's point of view. (See Note)

Note: The criteria is whether an operator can protect the operator's subscribers against location requests, which needs enhanced privacy check. The operator may reject a Rel-4 location request in a Rel-5 network.
~~The Rel-5 GMLC includes a notification to HLR that it supports enhanced user privacy.~~

SGSN/MSC	Rel-5	Rel-4 or earlier	Rel-5
HLR	Rel-5	Rel-5	Rel-5
GMLC which received the location request from LCS client	Rel-4 or earlier	Rel-5	Rel-5
7.1 PPR attached to GMLC	Yes If the operator wants to protect operator's subscriber against unwelcome location request, HLR needs to reject SRI from the GMLC because the enhanced privacy cannot be checked. HLR may reject SRI from the GMLC depending on the setting in HLR The GMLC cannot access the PPR	Yes Enhanced privacy check is performed in the PPR and the PPR rejects the unwelcome location request. GMLC will use in PSL request to MSC a Pseudo LCS Client ID that it receives from the PPR to provide backward compatibility	Yes Enhanced privacy check is performed in the PPR and the PPR rejects the unwelcome location request.
7.2 PPR attached to MSC/SGSN	Yes Rel-4 privacy checks remain in MSC/SGSN and are possible If the operator wants to protect operator's subscriber against unwelcome location request, HLR needs to reject SRI from the GMLC because the GMLC cannot send some parameters for enhanced privacy to the MSC/SGSN and the MSC/SGSN cannot check the enhanced privacy by using new parameters (i.e. codeword, requestor id, service type, etc) The MSC/SGSN can access the PPR, but the MSC/SGSN cannot obtain some parameters sent from the LCS client because the GMLC does not support Rel-5.	Yes, the HLR may reject the SRI if the MSC/ SGSN does not support the proper LCS capability set. The Pseudo Id cannot be used. The MSC/SGSN cannot access the PPR and rejects the request due to Rel-4 incompatibility reasons.	Yes Enhanced privacy check is performed in the PPR and the PPR rejects the unwelcome location request.
7.3 Home GMLC	Yes If the operator wants to protect operator's subscriber against unwelcome location request, HLR needs to reject SRI from the GMLC because the enhanced privacy cannot be checked. The GMLC cannot access the Home GMLC and SGSN/MSC	Yes Pseudo Id are used towards Rel-4 MSC/SGSN. Enhanced privacy check is performed in the Home GMLC and the Home GMLC rejects the unwelcome location request.	Yes Enhanced privacy check is performed in the Home GMLC and the Home GMLC rejects the unwelcome location request.

	SGSN/MSC.		
7.4 PPR- HSS	NA	NA	NA
Chapter 6 ~~7.5~~ Rel-4 architecture	Yes If the operator wants to protect operator's subscriber against unwelcome location request, HLR needs to reject SRI from the GMLC because the enhanced privacy cannot be checked. HLR may reject SRI from the GMLC depending on the setting in HLR, so the GMLC could not access the SGSN/MSC	Yes HLR may reject SRI if the MSC/SGSN does not support the proper LCS capability set.	Yes Codeword is checked in the ~~HLR~~ GMLC in HPLMN and the HLR rejects the requests if the codeword check is not performed~~successful~~ or the MSC/SGSN does not support proper capabilities

Table 7.5.2; Other criteria

Note: The Network Scenario for this table is that GMLC, HLR, MSC/SGSN are all Release 5 (except column 2).

	Enhanced support for location information privacy in other services e.g. Presence and Generic User Profile	The operator can provide the enhanced Rel-5 privacy mechanisms to the Target UE subscriber or not in the Rel-4 MSC/SGSN	Call/Session related Class (Note 2)	Deferred MT-LR (Note 3) Handling of event-based LCS (Note 4)
7.1 PPR attached to GMLC	FFS	Yes for enhanced privacy check in network. The operator can provide the en-hanced privacy mechanism even if the MSC/ SGSN is Rel-4 using pseudo id. No in the sense that codeword, service type, requestor are not shown to target UE.	Yes PPR can send two results: - call/session unrelated and - call/session related MSC/SGSN shall confirm if the request is call/session related	Yes VMSC/SGSN might have to contact PPR in the HPLMN (depending on the event), carrying the information needed to perform privacy checks.
7.2 PPR attached to MSC/SGSN	FFS	Yes for codeword check in HLR No for other enhanced privacy checks. No in the sense that codeword, service type, requestor are not shown to target UE.	Yes MSC/SGSN recognize the call/session related connections and can support it for the enhanced services	Yes VMSC/SGSN might have to contact PPR in the HPLMN (depending on the event), carrying the information needed to perform privacy checks.
7.3 Home GMLC	FFS	Yes for enhanced privacy check in network. The operator can provide the enhanced privacy mechanism	Yes Call/Session related class is handled in SGSN/MSC. Home GMLC may replace the external client identity to the pseudo external	Yes When the enhanced privacy setting of the UE is changed, the Home GMLC cancels the deferred MT-LR dependent on the

		privacy mechanism even if the MSC/ SGSN is Rel-4 using pseudo ids No in the sense that codeword, service type, requestor are not shown to target UE.	to the pseudo-external client identity.	dependent on the changes.
7.4 PPR-HSS	NA	NA	NA	NA
~~7.5~~ Chapter 6 Rel-4 architecture	FFS	Yes for codeword check at GMLC in HPLMN ~~in HLR~~ No for other enhanced privacy checks. No in the sense that codeword, service type, requestor are not shown to target UE.	Yes (no impact)	Yes (no impact for deferred LR) For event based LR the VMSC/SGSN can perform privacy checks when the event occurs, basing on the event related information and SLPP. The SLPP would need to be updated.

Note 2: The criteria is whether it is possible to handle the call/session related class in SLPP that is already defined in Rel-4 sSpecifications and to be enhanced for the Rel-5 privacy settings. If the PPR or Home GMLC does not stores the SLPP and the SLPP is checked in the MSC/SGSN, this issue is not caused.

Note 3: The criteria is whether it is possible to reflect the new privacy setting changed during waiting the event occurrence of the deferred MT-LR.

Note 4: In deferred location request the privacy check has to be performed when the event occurs. The criteria is the possibility to handle event-based LCS: for some events, the result of the privacy checks may depend on information owned by the VPLMN. When such new events are defined, the information has to be transferred to the node performing privacy checks. If privacy checks are performed in the HPLMN, the interfaces between the VPLMN and HPLMN have to be updated for each new privacy check. This shows that if the privacy checks are performed in the HPLMN, there will be anyway the need to update interfaces when new privacy checks are introduced.

The description of the architecture alternatives might need to be changed to show how the privacy of deferred location requests is handled.

~~Editor's note: Table 7.5.3 below is the same as in version 1.1.0 of this TR. The discussion is still to be continued regarding this table.~~

Table 7.5.3; Other differences between architecture alternatives

	Interface that is new or affected	Enhanced privacy check	SLPP check in MSC/SGSN	Impacts on the network due to migration from Rel-4 to Rel-5
7.1 PPR attached to GMLC	New Lr: FFS Affected Lh, Lg	PPR contains and checks both the enhanced privacy settings and the legacy privacy settings.	MSC/SGSN may check the SLPP according to the operator's policy.	New node to be introduced. New interface to be defined. Already existing function removed from existing nodes.
7.2	New	PPR contains and checks both the	MSC/SGSN may check the SLPP	New node to be introduced. New

PPR attached to MSC/SGSN	Ld: FFS Lt: FFS Affected Lg, HLR-MSC/SGSN (PPR address)	checks both the enhanced privacy settings and may contain the legacy privacy settings.	check the SLPP according to the operator's policy.	introduced. New interfaces to be defined.
7.3 Home GMLC	New Lr: FFS Affected Lh	Home GMLC contains and checks only the enhanced privacy settings. Legacy privacy check in Home GMLC is FFS.	MSC/SGSN always checks the SLPP.	Existing node impacted. Interface to be defined.
Chapter 6 Rel-4 architecture	New NONE Affected Lh,Lg, HLR-MSC/SGSN	GMLC in HPLMN owns and checks the codeword. Service type is checked in the MSC/SGSN	MSC/SGSN always checks the SLPP.	Small impacts (only few new parameters) on existing nodes and interfaces as a normal function upgrade.

	~~Interface that is new or affected.~~	~~Enhanced privacy check.~~	~~SLPP check in MSC/SGSN~~	~~Other features?~~
~~7.1 PPR attached to GMLC~~	~~New~~ ~~Lr: FFS~~ ~~Affected~~ ~~Lh, Lg~~	~~PPR contains and checks both the enhanced privacy settings and the legacy privacy settings.~~	~~MSC/SGSN may check the SLPP according to the operator's policy.~~	
~~7.2 PPR attached to MSC/SGSN~~	~~New~~ ~~Ld: FFS~~ ~~Lt: FFS~~ ~~Affected~~ ~~Lg~~	~~?~~	~~?~~	
~~7.3 Home GMLC~~	~~New~~ ~~Lr: FFS~~ ~~Affected~~ ~~Lh~~	~~Home GMLC contains and checks only the enhanced privacy settings.~~ ~~Legacy privacy check in Home GMLC is FFS.~~	~~MSC/SGSN always checks the SLPP.~~	
~~7.4~~	~~New~~ ~~?~~			

	~~Affected~~ ~~?~~			

7.~~6~~7 Conclusion on architecture for the enhanced privacy checking

~~Editor's note: The content of this chapter is not yet agreed.~~

See chapter 13, Conclusion.

8. Possible requestor enhancements in Rel-6 ~~Stage 2 description of Requestor indication~~

In Rel-6 the requestor concept could be further enhanced by introducing a so-called "Authorized Requestor List". The "Authorized Requestor List" is defined by the target user and not by the operator as for the "Authorized UE List". The "Authorized Requestor List" may be used to control the access to location information even though the user is not subscribing to notification/verification, but still wants to control what requestors can get his location.

TS 23.271 pre-Rel-5 defines a LCS Location Notification Invoke message sent to the target UE in a MT-LR both in the CS and the PS domain. This message indicates the type of location request and the identity of the LCS client and whether privacy verification is required. From target UE user point of view this reflects only part of the location request chain, i.e. a possible requesting entity remains unknown to the target UE user. This is considered as a flaw in terms of target UE user privacy in pre-Rel-5.

The identities of the r~~R~~equestor can be e.g. MSISDNs or logical names. ~~Editorial note:~~ The requestor identity need perhaps not be globally unique, comp papa and Naomi.

The LCS Location Notification procedure should be enhanced for transferring the rRequestor identity to the target UE for a case-by-case authorization by the user.

Functional r~~R~~equirements:

- The requestor identity should be added as an information element to be carried on the Le, Lg and Lc interfaces.
- The requestor identity should be included in the location request, if available. When the originator of a location request is the LCS client itself, the LCS client may set the LCS client name as the requestor identity.
- When there is the originator as an independent entity of the LCS client and the LCS client does not have the requestor identity corresponding to the location request, some special value may be sent as the requestor identity. (The special value may be "empty".) The actual value of the special value is outside the scope of the present document.
- Before the LCS client issues a location request on behalf of a requestor, the requestor identity shall be duly authenticated so that the target user can trust the displayed requestor name to be correct.
- The requestor identity should be added to the LCS Location Notification Invoke procedure

~~Note: Anonymous location request is for further study.~~

8.1 Architecture alternative with requestor authentication in GMLC

Figure 8.1 illustrates the MT-LR signaling procedure when the requestor identity is authenticated in GMLC.

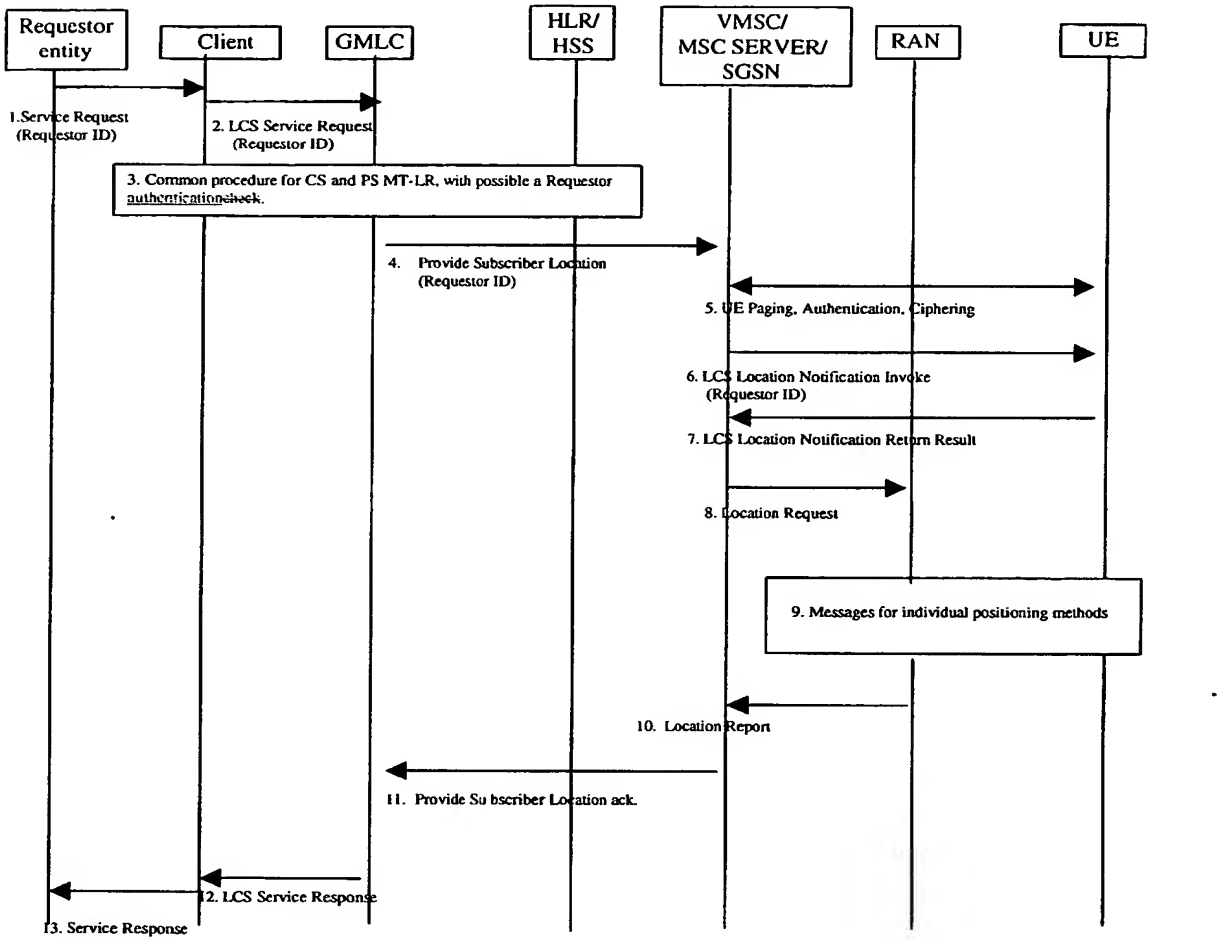

Figure 8.1; MT-LR signaling procedure when the requestor identity is authenticated in GMLC

1) A requestor entity is accessing an LCS Client requesting a service, which requires the location information of a target UE. {The interface rRequestor – LCS client is outside the scope of this TR.} The identity of the rRequestor may be added to the service request by the requestor. Another possibility is that the rRequestor identity is obtained from the LCS Client as the requestor is authenticated with the LCS Client. In this case the rRequestor identity also needs to be provisioned in the privacy profile.

Note: According to this description, the requestor identity may be authenticated both by the LCS client and the GMLC in this case.

2) The LCS Client issues a location request to the GMLC containing the identity of the rRequestor.

3) Common PS and CS MT-LR procedure as described in 23.271 section 9.1.1. After the authentication of the LCS Client and checking that the target UE is on the "Authorized UE List", the "Allowed Requestor List" is checked for authorization of the location request for this rRequestor.

Note: More detailed description of steps 4 to 12 can be found in TS 23.271, section 9.1.2 onwards.

4) The GMLC sends a PROVIDE_ SUBSCRIBER _LOCATION message to the MSC/MSC server/SGSN indicated by the HLR/HSS. This message carries also the new rRequestor iIdentity information. If the target UE subscriber profile so indicates, the UE must be notified for privacy verification. The rRequestor identity is included in the LCS Location Notification Invoke message together with the LCS Client Id.

5) Described in 23.271 section 9.1.2.

6) If the location request comes from a value added LCS client and the UE subscription profile indicates that the UE must either be notified or notified with privacy verification and the UE supports notification of LCS (according to the UE Capability information), an LCS Location Notification Invoke message is sent to the target UE indicating the type of location request (e.g. current location) and the identity of the LCS client, rRequestor identity and whether privacy verification is required.

7) to 12) Described in 23.271 section 9.1.2

13) The LCS Client sends the service response back to the requestor with the location information of the target UE. In case there was an error or the request was denied or not authorized this may be indicated in the service response. However, specification of the service response is outside the scope of this TR.

8.2 Architecture alternative with requestor authentication in the LCS client

Figure 8.2 illustrates the MT-LR signaling procedure when the requestor identity is authenticated in the LCS client.

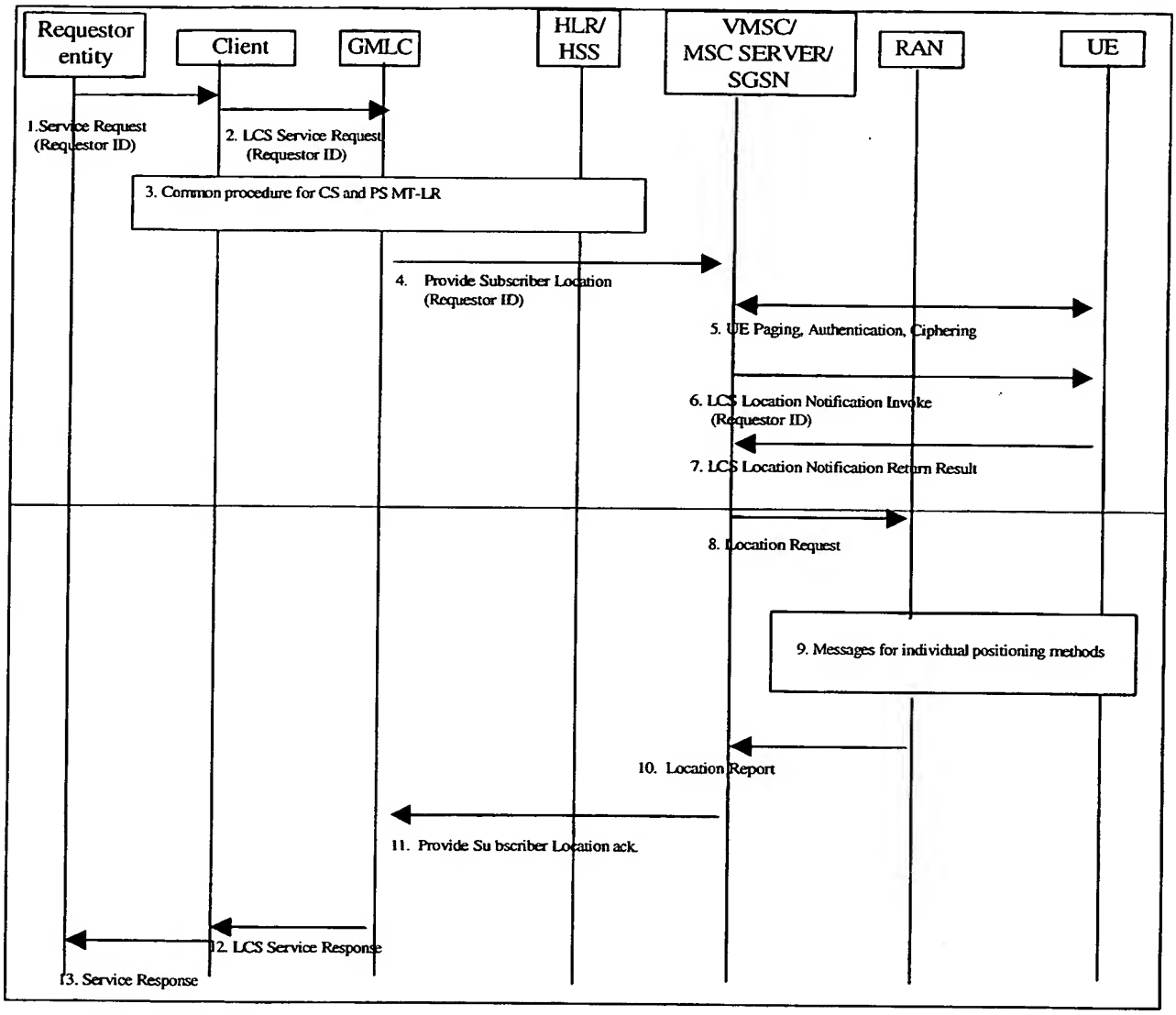

Figure 8.2: MT-LR signaling procedure when the requestor identity is authenticated in the LCS client

1)A requestor entity is accessing an LCS Client requesting a service, which requires the location information of a target UE. [The interface Requestor – LCS client is outside the scope of this TR.] The identity of the Requestor may be added to the service request by the requestor. Another possibility is that the Requestor identity is obtained from the LCS Client as the requestor is authenticated with the LCS Client.

2)The LCS Client issues a location request to the GMLC containing the identity of the Requestor.

3)Common PS and CS MT-LR procedure as described in 23.271 section 9.1.1.

Note: More detailed information of steps 4 to 12 can be found in TS 23.271 section 9.1.2 onwards.

4)The GMLC sends a PROVIDE_SUBSCRIBER_LOCATION message to the MSC/MSC server/SGSN indicated by the HLR/HSS. This message carries also the new Requestor Identity information. If the target UE

~~subscriber profile so indicates, the UE must be notified for privacy verification. The Requestor identity is included in the LCS Location Notification Invoke message together with the LCS Client Id.~~

~~5) Described in 23.271 section 9.1.2.~~

~~6) If the location request comes from a value added LCS client and the UE subscription profile indicates that the UE must either be notified or notified with privacy verification and the UE supports notification of LCS (according to the UE Capability information), an LCS Location Notification Invoke message is sent to the target UE indicating the type of location request (e.g. current location) and the identity of the LCS client, Requestor identity and whether privacy verification is required.~~

~~7) to 12) Described in 23.271 section 9.1.2~~

~~13) The LCS Client sends the service response back to the requestor with the location information of the target UE. In case there was an error or the request was denied or not authorized this may be indicated in the service response. However, specification of the service response is outside the scope of this TR.~~

8.~~3~~2 Backward compatibility

MSC, SGSN and UE according to previous releases do not support the requestor functionality.

When a location request is passed through MSC, SGSN or GMLC of previous releases, the requestor identity of the location request may be dropped and UE may not be able to receive the identity.

When a Rel-5 LCS client or Rel-5 GMLC is going to send a location request and the client or the GMLC does not have a requestor identity, which corresponds to the location request, the client or the GMLC should send some special value as the requestor identity of the request. (Note: The actual value of the special value is outside the scope of this TR~~the present document~~.) When a location request, expected to contain the requestor identity, is notified to the UE without requestor identity, the UE is able to judge that the requestor identity was dropped due to the lack of network capability.

~~As an alternative, the requestor identity could be carried as part of the LCS client name. In this case, when an LCS client name, expected to contain the requestor identity, is notified to a Rel-5 UE without the requestor identity, the UE is able to judge that the requestor identity was not provided from the LCS client. But this alternative is for further study.~~

~~9. Stage 2 description of the codeword concept~~

~~There are three ways to standardize the codeword handling. One way is that the codeword is stored in the GMLC and compared in the GMLC. Another way is that the codeword is stored in the PPR and compared in the PPR. A further solution is that the codeword is stored and compared in the HLR. These alternatives are described and compared in chapter 7.~~

~~10.~~9. Stage 2 description of the anonymity concept

The stage 2 description is FFS.

~~11. Common stage 2 privacy issues in Presence and Location services~~

~~The Presence service may act as a LCS client and request location information from GMLC. The location request and privacy are handled as specified in 23.271 for this LCS client.~~

~~The Presence service itself may request from the location server what are the privacy settings that shall be applied for the location information of the target mobile before forwarding location information or other presence attributes to other parties.~~

~~Possible differences between privacy settings in presence and in LCS should be resolved.~~

1012. Charging Aspects

No charging aspects have been identified.

1113. Security aspects

The following security aspects and security requirements have been identified:

- It shall be possible to verify that the service identity indicated by the LCS client is correct. The service types offered by a certain LCS Client is to be part of the LCS Client service profile, which shall be known by the GMLC. An LCS client is hence not able to claim to offer services that are not included in its profile.
- The service type should only be conveyed between PLMNs with valid roaming agreements.
- The requestor should be authenticated by the LCS client.
- According to current specifications the LCS client shall be authenticated by GMLC and authorized based on information in HLR.
- The alias for an anonymous target mobile or for an anonymous requestor shall be generated in a secure way, such that the real identity is never revealed to a third party.

SA1 has specified service requirements for the requestor, LCS client, LCS server and e.g. requirements to protect the privacy of the target mobile user. The security aspects of LCS are specified in TS22.071, chapter 4.7.

1214. Roaming, Service Availability and Continuity

There is a Work Item in the Rel-6 time frame regarding a new GMLC – GMLC interface to improve roaming support.

13. Conclusion

In Rel-5 few new service requirements for LCS have been identified i.e. "Codeword", "Service Type" and "Requestor". All these three concepts have been handled and included in Rel-5 LCS stage 2 TS (v. 5.2.0) by means of minor functional requirements on the existing architecture, without any need of new architecture.

The current LCS stage 2 TS is also in line with the existing Rel-5 service requirements concerning the privacy of roaming subscribers and allows protecting their privacy with Rel-5 mechanisms. In fact the HPLMN is aware of the LCS capabilities of the VMSC/SGSN by means of "Supported LCS capabilities sets" mechanism: the HPLMN (HLR/HSS) is aware of the VMSC/SGSN capability to support Rel-5 privacy checks and can have the full control in order to protect the privacy of subscribers roaming in a different PLMN. This means that if the VPLMN does not support Rel-5 privacy checks, the HLR may reject the LCS request, without any involvement of the VPLMN and/or useless signalling.

A change in the architecture can be proposed in next releases when new service requirements that are not feasible to be implemented in the existing architecture are identified. The LCS network architecture in Rel-6 will take into account the GMLC-GMLC interface and will be guided by identified Rel-6 service requirements.

The Technical Report will not be continued in Rel-6, instead the Rel-6 solutions will be discussed and agreed based on proposed CRs against LCS stage 2 specification 23.271.

Annex A (informative): Change history

Ver. 0.0.1	October 26, 2001	First Draft
Ver. 0.0.2	October 31, 2001	Comments added in SA2 #20 LCS drafting
Ver. 0.0.3	November 1, 2001	Password functionality added
Ver. 0.1.0	November 2, 2001	Version number raised to 0.1.0
Ver. 0.2.0	December 3, 2001	Contributions and comments added in SA2#21
Ver. 0.3.0	December 10, 2001	e-mail comments added
Ver. 0.4.0	December 11, 2001	Siemens' e-mail comments added
Ver.1.0.0	December 16, 2001	For information to SA#14. Same technical content as v.0.4.0
Ver. 1.1.0	January 23, 2002	Changes and addition as agreed in SA1 LCS SWG and SA2#22 LCS session, Phoenix, U.S.A.
Ver. 1.2.0	February 25, 2002	Changes and addition as agreed in SA2#23 LCS session, Sophia-Antipolis, France
Ver. 2.0.0	March, 2002	V.2.0.0 created for submission at TSG SA#15. Same technical content as v.1.2.0
Ver. 2.1.0	April 29, 2002	Changes and addition as agreed in SA2#24 LCS session, Madrid, Spain

Change history							
Date	TSG #	TSG Doc.	CR	Rev	Subject/Comment	Old	New
					V.2.0.0 created for submission at TSG SA#15. Same technical content as v.1.2.0	1.2.0	2.0.0